CRIPTOMONEDAS

Hackers se roban 550 mil dólares en criptomonedas con ataque masivo

El Ciudadano · 5 de junio de 2018

Los expertos señalan que la incursión se realizó con una poderosa granja de minería y que probablemente fueron alquiladas otras para cometer el desfalco

Un grupo de hackers realizó un ataque masivo a ZenCash, que permitió tomar el control del 51% dela red de control de registro de la cadena y apoderarse con 550 mil dólares en criptomonedas mediante transacciones dobles contra casas de cambio.

El comunicado de la empresa ZenCash explica que el ataque se realizó el domingo y ya el equipo de desarrollo implementó medidas y contactó con otras casas de cambio para realizar una investigación a fondo sobre las transacciones sospechosas.

El monto en criptomonedas robados fue con transacciones dobles de 6.600 y 13.000 ZEN, que equivalen a 550 mil dólares.

Criptonoticias

Las investigaciones preliminares apuntan a dos hipótesis: el atacante tiene una poderosa granja de criptomonedas o alquiló el poder de procesamiento para comprometer los algoritmos de ZenCash.

Sin embargo el peligro radica en el procedimiento usado por los hackers para vulnerar la red. En el comunicado explican que el algoritmo de minado es Equihash, que también es usado por Bitcoin Gold, Zclassic y Bitcoin Private, por que ya las empresas fueron avisadas para evitar posibles fugas futuras.
Un portal especializado en el cálculo de este tipo de ataque, informó que los hacker posiblemente invirtieron cerca de 7 mil dólares.

Entre las recomendaciones que divulgó ZenCash a las otras casas de cambio, es elevar al máximo el número de confirmaciones requeridas para todas las transacciones y así evitar que los hackers se hagan con el control.

El Ataque

La empresa detalló que el ataque se efectuó desde varias granjas de criptomonedas, propias o alquiladas, y fue dirigido a una cadena particular de blockchain lo que permitió hacerse con el registro del 51% de ZenCash.

Este poder de procesamiento permitió al agresor, revertir y anular transacciones ya realizadas por las casas de cambio al tener el control de los bloques. Las cadenadas de transacciones minadas pueden ser manejadas a voluntad sin que parezcan fraudulentas, por lo que los sistemas la asumen como válida.

Fuente: El Ciudadano